



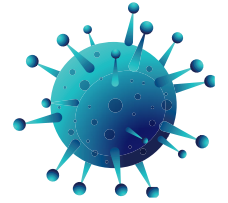
**GUIDE ON
DATA PROTECTION FOR
HEALTH DATA
AND
ARTIFICIAL INTELLIGENCE
SOLUTIONS**

**IN THE CONTEXT OF THE
COVID-19 PANDEMIC**

Issued by the Data Protection Office

17 April 2020

Data Protection and Coronavirus (COVID-19)



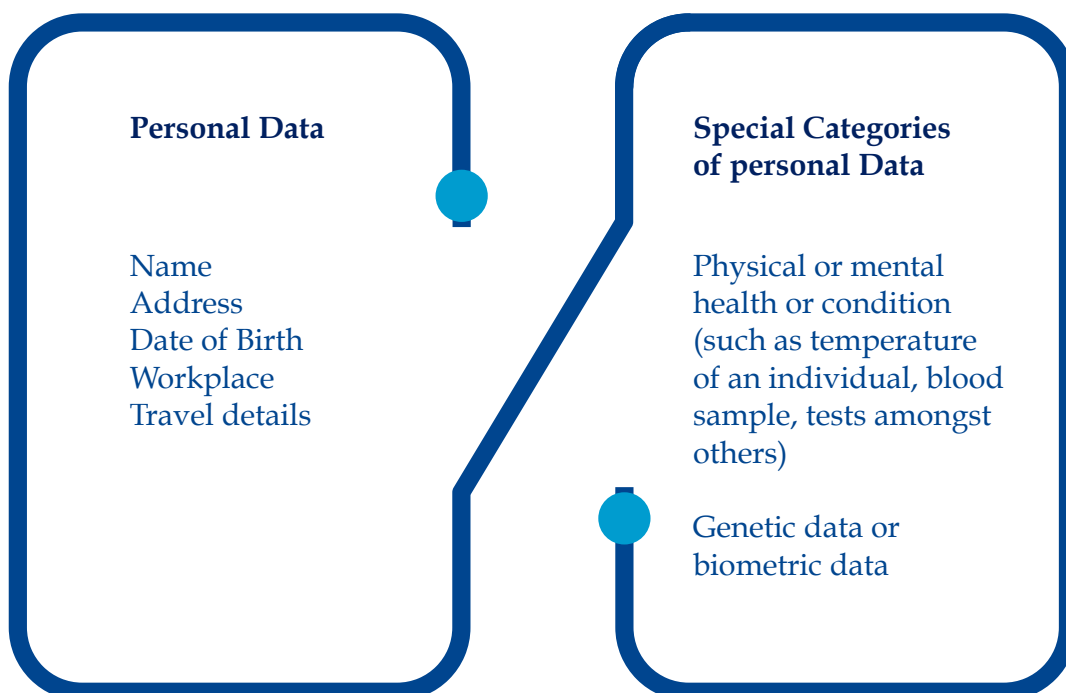
The Data Protection Office recognises the unprecedented challenges that Mauritius and other countries in the world are facing during the COVID-19 pandemic. While it is clear that data protection rights are not absolute and can in no way be a barrier to save human lives, it is equally crucial to reiterate that the fundamental rights to privacy and data protection are still applicable.

To contain the spread and mitigate the effects of COVID-19, necessary steps are being taken by governments as well as public, private and voluntary organisations around the world. It is worth mentioning that the techniques for containing the COVID-19 virus are various in different jurisdictions. However, many of these methods process personal data (such as name, address, travel details, workplace) of individuals including in many cases special categories of personal data such as health data (temperature, blood sample, amongst others).

The processing of personal data and special categories of personal data implies that the Data Protection Act (DPA) 2017 applies in this crisis situation. Organisations whether public or private in Mauritius should continue to comply with the requirements set out in the DPA. The essence of all decisions resides on knowing what we do, its outcome(s) and acting when it is necessary and proportionate to do so. The underlying principle of necessity and proportionality must be at the basis of all legitimate objectives pursued. Appropriate safeguards must also be embedded to protect an individual's rights.

To start with, when considering any control, organisations must:

1. Identify the types of personal data being processed



2. Identify the lawful basis for processing

There is a number of legal basis for the processing of personal data under section 28 of the DPA, and stricter conditions permitting the processing of special categories of personal data, such as health data, under section 29 of the DPA. In other words, consent of an individual is **not** the **only** legal ground that allows for the lawful processing of personal data. If an organisation satisfies any other legal basis provided under the DPA apart from consent, the processing will be considered as lawful.

If the processing concerns only personal data (e.g. name, address, telephone number), then section 28 of the DPA must be complied with.

Section 28 - Lawful processing

(1) No person shall process personal data unless–

- (a) the data subject consents to the processing for one or more specified purposes;
- (b) the processing is necessary–
 - (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
 - (ii) for compliance with any legal obligation to which the controller is subject;
 - (iii) in order to protect the vital interests of the data subject or another person;
 - (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (v) the performance of any task carried out by a public authority;
 - (vi) the exercise, by any person in the public interest, of any other functions of a public nature;
 - (vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
 - (viii) for the purpose of historical, statistical or scientific research.

In case the processing concerns personal data (e.g. name, address, telephone number) and special categories of personal data, then both sections 28 and 29 of the DPA must be complied with.

Section 29 - Special categories of personal data

Special categories of personal data shall not be processed unless –

- (a) section 28 applies to the processing; **and**
- (b) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (c) the processing relates to personal data which are manifestly made public by the data subject; or
- (d) the processing is necessary for–
 - (i) the establishment, exercise or defence of a legal claim;
 - (ii) the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2);
 - (iii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or
 - (iv) protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

Examples:

a) Processing the names, addresses, telephone numbers and health data of patients by the Ministry of Health and Wellness

In this case, the Ministry can rely on the following legal basis stipulated under the DPA 2017 for the processing where consent of the data subjects (patients or individuals) will not be required.

Section 28 (1)(b)(ii)

For compliance with any legal obligations such as the Public Health Act

Section 28 (1)(b)(iv)

For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

AND

Section 29 (1)(d)(ii)

For the purpose of:

1. preventive and occupational medicine,
2. for assessing the working capacity of employees,
3. for the provision of health or social care or treatment or management of health or social care systems

Section 29 (1)(d)(iii)

For carrying out the obligations and exercising specific rights of the controller or of the data subjects

Section 29 (1)(d)(iv)

For protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent

b) Employers

In Mauritius, the Occupational Safety and Health Act 2005 provides legal obligations for an employer to ensure the safety, health, and welfare at work of all his employees as far as is reasonably practicable. Therefore, employers may rely on:

Section 28 (1)(b)(ii) - For compliance with any legal obligations

Section 28 (1)(b)(vii) - Legitimate interests of the controller or third party

And

Section 29(1)(d)(iii) - the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject

Note: Employers should not disclose personal data of employees who have contracted the COVID-19. Thus, care should be taken when communicating the presence of COVID-19 in the workplace.

c) Taking of body temperature of individuals by staff at the entrance of hypermarkets/supermarkets/superettes in Mauritius until 04 May 2020

In Mauritius, to contain the spread of the Coronavirus, the Minister of Health and Wellness has issued the general notice No. 562 of 2020 under the Public Health Act under regulation 16(1) of the Prevention and Mitigation of Infectious Disease (Coronavirus) Regulations 2020. In this context, the legal basis of processing temperature by hypermarkets/supermarkets/superettes until 04 May 2020 are as follows:

Section 28(b)(ii) for compliance with any legal obligation to which the controller is subject;

Section 29 (d)(iii) the purpose of carrying out the obligations and exercising specific rights of the controller

Note:

Organisations must make a **judicious** assessment regarding the legal basis for any envisaged processing based on circumstances of the processing to avoid any undue infringement to the privacy rights of individuals. Consent of individuals will be required when no other legal basis for processing personal data is applicable.

3. Apply the data minimisation principle

Organisations must only collect and process personal data that is required and not excessive to prevent or contain the spread of COVID-19 in accordance with section 21 (c) of the DPA.

4. Be transparent

Organisations must be transparent regarding the measures they implement in this context, including the purpose/s of collecting the personal data, the intended recipients of the data and how long it will be retained at the time of collection through the display of appropriate notices. They must provide individuals with information regarding the processing of their personal data in a format that is concise, easily accessible, easy to understand, and in clear and plain language as per sections 23 and 37(2) of the DPA.

5. Ensure appropriate security controls are in place

According to section 31 of the DPA, organisations must implement appropriate security and organisational measures to protect personal data. Therefore, any data processing in the context of COVID-19 must be carried out in a manner that ensures the confidentiality of individuals and security of the data, in particular where health data is concerned. Access to data must be limited to authorised persons only.



The identity of individuals **should not be disclosed** to any third party or their colleagues without a clear justification.

Some broad organisational measures that controllers may take to prevent the spread of the COVID-19 are:

- Disinfection and workspaces should be thoroughly cleaned, sanitised and ventilated.
- Wearing of face masks
- Apply social distancing rules (avoid face to face meetings).
- All common areas including door handles/office spaces, amongst others, should be cleaned regularly and disinfected.
- Provide hand washing and hand sanitisation facilities around sensitive locations (e.g lifts, doors, photocopy machines, canteens, toilets, mess rooms, amongst others).

6. Record of processing operations

Organisations should also ensure that they document any processing of personal data regarding measures implemented to manage COVID-19.

Artificial Intelligence (AI)

In light of the unprecedented turmoil and challenges that the world is facing due to the spread and death tolls linked to the COVID-19, many governments around the world are exploring and applying Artificial Intelligence solutions to contain and forecast the spread of the virus besides the application of lockdown measures and limitations of movement. AI solutions require the processing of huge amounts of data to learn and make intelligent decisions. Governments are looking for opportunities for improved surveillance, monitoring and detection controls through the use of AI-technology driven tools.



AI is being widely used by different countries to fight the virus from all fronts from screening to diagnosis and to containment and drug development. AI is thus assisting health care personnel around the world to fight against COVID-19 virus.

In some countries, it is being observed that facial recognition technology is being used for tracking individuals who have travelled to affected areas. In other states, law enforcement authorities are using drones to broadcast audio messages to effectively control the movement of people outside their homes. The use of monitoring bracelets on people travelling from abroad are also being used to alert authorities if the concerned individuals move away from their quarantine location during the quarantine period. This type of technology uses a code which pairs up with a smartphone application and uses the strength of surrounding communications signals such as Wifi, Bluetooth and GPS to evaluate any change in an individual's location depending on the strength or weakness of various signals. Some airports are also planning the use of biometric screening systems using fever detecting cameras to measure exactly the temperature of a traveller standing in front of a border counter.

Whilst the world turns to technology to come out of this crisis situation, caution must be applied. The processing of personal data and special categories of personal data by AI- driven technologies must not distort an individuals' fundamental rights to privacy. It can vary across countries as different jurisdictions and laws come into play. Nevertheless, it is encouraged that a responsible use of AI technologies is adopted. There are different ways that can ensure a responsible use of AI in line with the basic principles of data protection laws such as :

1. Data anonymisation techniques

The use of anonymisation techniques must be encouraged when deploying AI solutions. The processing of anonymised data enables the study of the movement of large groups in a more general way.

2. Pseudonymisation techniques

Instead of capturing the exact identity of individuals and making it available to others especially for a COVID-19 positive patient, algorithms that use pseudonymisation must be encouraged so that relevant information is made available but which does not directly reveal the identity of individuals.

3. Purpose limitation

All personal data processed in the context of the spread of the COVID-19 and public health must not be re-used later for other incompatible purpose/s.

4. Transparency

The automated processing of data by AI solutions must be transparent to individuals. An individual must be made aware in simple ways regarding his/her relevant information being processed, the underlying logic and the significance and expected consequences of such processing. In other words, individuals must be provided with sufficiently comprehensive information to understand the reasons for any decisions derived from the processing.

5. Right to be informed

Individuals must be informed of the types of data being collected, the purpose/s of the processing, the organisations who will use the data and with whom it will be shared with and the duration that the data will be stored. Besides, individuals must be made aware of whether the processing of his/her personal data is voluntary or mandatory.

6. Time limitation

Although the battle against the COVID-19 is still ongoing and not yet to an end, it is vital that authorities work back and re-assess the technologies deployed at the end of the battle so that any undue infringement to the rights and privacy of individuals do not become the norm of future processing.

Software Development and Mobile Applications

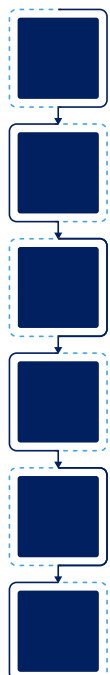
New software and mobile applications are being developed by various organisations around the world, mainly for contact tracing or proximity tracing purposes.

Similar to AI-driven technologies, mobile applications must comply with data protection principles such as proportionality, data minimisation and time limitation. Developers and organisations are encouraged to use privacy by design techniques when developing new software and applications.

Germany has an application for proximity tracing namely Pan European Privacy Proximity Tracing which informs the users whether they have been in the proximity of a person who was tested positive for COVID-19. The app uses pseudonymisation techniques as a security measure. It is to be noted that users have to provide their consent before the use of the application to participate in it.

Users of mobile applications must also be informed of how to discontinue/delete a mobile application afterwards so that no undue covert surveillance / monitoring is made when no longer required.

The Data Protection Office recommends software development organisations and application developers to observe the following:

- 
- 1 Collect only data that is required. Proportionality, data minimisation and other principles of the DPA should be observed.
 - 2 Use privacy by design techniques
 - 3 Ensure appropriate security measures are implemented
 - 4 Inform users of the purpose/s of any technology/software application
 - 5 Have a lawful basis for processing (consent or any other criteria as mentioned in sections 28 and 29 (if applicable) of the DPA)
 - 6 Consult the Office where necessary



Infringements of the DPA 2017

An individual reserves the right to lodge a complaint with the Data Protection Office for any infringement under the DPA 2017. Under section 43 of the DPA 2017, any person who commits an offence for which no specific penalty is provided or who otherwise contravenes the Data Protection Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Conclusion

Whilst the world is living a novel situation with the COVID-19 pandemic, it is crucial that we come out of it using best practices and recommended approaches. Privacy is an inborn human right while technology is man-made. We must do our best to combat the virus and at the same time preserve at most the privacy rights of individuals by adopting the correct approaches right from the design stages of any technology solution. The foundational principles of necessity and proportionality must also be followed coupled with appropriate safeguards to serve mankind.

Some Questions

1. Most of our staff will be working from home in the event of confinement. What process should we have in place for processing personal data such as payroll at home?

- The organisation will need to implement a procedure i.e. a remote working policy to outline clearly the conditions of remote work including the responsibilities of the employees. Responsibility is important when performing remote work, as you do not have a constant overview of the employees' performance of duties and cannot check them.
- The rules of data (including personal data) protection should be clearly stipulated in the remote working policy. In other words, the policy should cover the following matters: where the employees may take the computer and the employer's documents, what kind of IT- solutions can and must be used, where and how the documents must be kept and how to act when there is a risk of data leakage or a leak has occurred. You may request the employees to sign a confidentiality agreement.
- As per section 31 of the Data Protection Act 2017, a controller or processor shall, at the time of the determination of the means for processing and at the time of the processing implement appropriate security and organisational measures. Thus, you will need to ensure that:
 - Strong password systems are implemented. To do so,
 - Use strong passwords that are memorable, unique and unidentifiable.
 - Update the employees' login credentials frequently.
 - For further protection, enable two-factor authentication.
 - Reduce the number of login attempts to 3 attempts before blocking the login screen.
 - Proper access control is provided to each employee – Employees should have access to only data that they need in order to do their job.
 - A Virtual Private Network (VPN) is implemented to securely connect to a network for working remotely.
- Employees should be informed via the policy that using public Wi-Fi (in a café, shopping centre, amongst others) is not permissible. In case your employees have no other option but to use an unsecured network, make sure they use a VPN and limit file sharing.

2. Can I collect personal data as well as health data such as temperature in relation to COVID-19 for employees/visitors to control access in the organisation's premise?

- Organisations have a legal obligation to ensure the safety, health, and welfare at work of all its employees as far as is reasonably practicable under the Occupational Safety And Health Act 2005. Thus, they can rely on the exceptions set out in section 28 (1)(b)(ii) as well as section 28 (1)(b)(vii) which is on legitimate interest and section 29 (1)(d)(ii) or section 29 (1)(d) (iii) of the DPA for the processing of the personal data in relation to COVID-19.
- Note that in no circumstance can special categories of personal data be communicated without strict compliance with section 29 of the DPA either offline or online

3. Can I inform my staff that a colleague has contracted the virus?

- Yes you can inform your staff, however, don't provide the name of the individual.

4. Can I share the employees' health details to the authorities or Ministry of Health for treatment/health purposes?

- Yes, you may do so for any specific individual who has contracted the virus and who requires treatment from the Ministry of Health or private health institution. Data Protection Act won't stop you from doing so.

5. What considerations should we take when developing contact tracing apps?

- There are various considerations that must be looked at as elaborated in this guideline depending on the methodology being used and also on some other factors which may include, amongst others, information on whether:
 - It is a completely decentralised system where personal data is stored on the personal mobile which is controlled by the citizen?
 - The processing is totally anonymous?
 - It will be the user who will voluntarily disclose information if he has contracted the virus?